VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT Rec'd PCT/PTO 10 MAR 2005

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

REC'D 14 DEC 2004
WIPO PCT

Aktenzeichen des Anmelders oder Anwalts CPCT-12366	**WEITERES VORGEHEN** siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/EP 03/10015	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 09.09.2003	Prioritätsdatum *(Tag/Monat/Jahr)* 11.09.2002
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/30		
Anmelder GIESECKE & DEVRIENT GMBH et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 3 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Bescheids
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Regel 66.2 a)ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
02.03.2004	14.12.2004
Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Bevollmächtigter Bediensteter Liebhardt, I Tel. +31 70 340-4114

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP 03/10015

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung *(Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17))*:

Beschreibung, Seiten

1-19 in der ursprünglich eingereichten Fassung

Ansprüche, Nr.

1-13 eingegangen am 07.09.2004 mit Schreiben vom 07.09.2004

Zeichnungen, Blätter

1/4-4/4 in der ursprünglich eingereichten Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um:

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).

   ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

   ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:

   ☐ Ansprüche, Nr.:

   ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen.)

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-13
	Nein:	Ansprüche	
Erfinderische Tätigkeit (IS)	Ja:	Ansprüche	1-13
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (IA)	Ja:	Ansprüche:	1-13
	Nein:	Ansprüche:	

2. Unterlagen und Erklärungen:

   siehe Beiblatt

Zu Punkt V

Begründete Feststellung hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

Es wird auf das folgende Dokument verwiesen:

D1: WO 01/61918 A (SILVERBROOK RES PTY LTD ;WALMSLEY SIMON ROBERT (AU); LAPSTUN PAUL) 23. August 2001 (2001-08-23)

1. Das Dokument D1 wird als nächstliegender Stand der Technik gegenüber dem Gegenstand des Anspruchs 1 angesehen. Es offenbart ein Verfahren zum geschützten Ausführen einer kryptographischen Berechnung, bei der ein Schlüssel mit mindestens zwei Schlüsselparametern (Seite 69, Zeile 4, "K_1" und "K_2") herangezogen wird, wobei bei dem Verfahren eine Integritätsüberprüfung des Schlüssels durchgeführt wird (Seite 69, Zeilen 4-9), um einen kryptographischen Angriff zu verhindern, bei dem durch eine Verfälschung mindestens eines ersten Schlüsselparameters Rückschlüsse auf mindestens einen zweiten Schlüsselparameter gezogen werden.

   Der Gegenstand des Anspruchs 1 unterscheidet sich daher von dem bekannten Verfahren dadurch, daß mindestens ein Schlüsselparameter das Produkt eines für die kryptographische Berechnung benötigten Wertes mit einem Sicherungswert ist, und daß die Integritätsüberprüfung eine Teilbarkeitsprüfung beinhaltet.

   Der Gegenstand des Anspruchs 1 ist somit neu (Artikel 33(2) PCT).

   Die mit der vorliegenden Erfindung zu lösende Aufgabe kann somit darin gesehen werden, daß die mehrfache Durchführung der aufwendigen Berechnung der HMAC-SHA1-Prüfsumme gemäß Dokument D1 umgangen werden soll.

   Die in Anspruch 1 der vorliegenden Anmeldung für diese Aufgabe vorgeschlagene Lösung beruht aus den folgenden Gründen auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT):

   Die Aufgabe der Vermeidung der rechenintensiven HMAC-SHA1-Prüfsummen-berechnung wird im Dokument D1 nicht einmal andeutungsweise angesprochen.

Das Dokument D1 offenbart nicht die Tatsache, daß mindestens ein Schlüsselparameter das Produkt eines für die kryptographische Berechnung benötigten Wertes mit einem Sicherungswert ist, und daß die Integritätsüberprüfung eine Teilbarkeitsprüfung beinhaltet. Auch wird kein Hinweis auf diese Art der Integritätsüberprüfung gegeben, obwohl sie eine Vermeidung der rechenintensiven HMAC-SHA1-Prüfsummenberechnung bewirkt, daß die den Schlüsselparametern und Sicherungswerten inhärenten mathematischen Beziehungen genutzt werden und so eine Teilbarkeitsprüfung an Stelle der Prüfsummenberechnung zur Integritätsüberprüfung ausreicht.

2. Für die unabhängigen Ansprüche 12 und 13, die sich auf ein Computerprogrammprodukt beziehungsweise auf eine Chipkarte zur Ausführung des Verfahrens gemäß dem Anspruch 1 beziehen, gelten die obigen Überlegungen entsprechend. Besagte Ansprüche sind somit ebenfalls neu (Artikel 33(2) PCT) und beruhen ebenfalls auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT).

3. Die Ansprüche 2-11 sind vom Anspruch 1 abhängig und erfüllen damit ebenfalls die Erfordernisse des PCT in bezug auf Neuheit und erfinderische Tätigkeit.

Patentansprüche

1. Verfahren zum geschützten Ausführen einer kryptographischen Berechnung, bei der ein Schlüssel (12) mit mindestens zwei Schlüsselparametern (p, q, pinv, sp, dp, sq, dq) herangezogen wird, wobei bei dem Verfahren eine Integritätsüberprüfung (30, 34, 40, 54) des Schlüssels (12) durchgeführt wird, um einen kryptographischen Angriff zu verhindern, bei dem durch eine Verfälschung mindestens eines ersten Schlüsselparameters (p, q, pinv, sp, dp, sq, dq) Rückschlüsse auf mindestens einen zweiten Schlüsselparameter (p, q, pinv, sp, dp, sq, dq) gezogen werden, dadurch **gekennzeichnet, daß** mindestens ein Schlüsselparameter (dp, dq) das Produkt eines für die kryptographische Berechnung benötigten Wertes mit einem Sicherungswert (sp, sq) ist, und daß die Integritätsüberprüfung (30, 34, 40, 54) eine Teilbarkeitsprüfung beinhaltet.

2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß der Sicherungswert (sp, sq) als Schlüsselparameter in dem Schlüssel (12) enthalten ist.

3. Verfahren nach Anspruch 1 oder Anspruch 2, dadurch **gekennzeichnet**, daß die kryptographische Berechnung ein RSA-CRT-Verfahren ist und daß der für die kryptographische Berechnung benötigte Wert ein CRT-Exponent ist, wobei das Produkt dieses CRT-Exponenten mit dem Sicherungswert (sp, sq) als gesicherter CRT-Exponent (dp, dq) in dem Schlüssel (12) enthalten ist.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch **gekennzeichnet**, daß bei der Integritätsprüfung (30, 34, 40, 54) geprüft wird, ob ein Schlüsselparameter (p, q, pinv, sp, dp, sq, dq) oder ein Wert, der sich von dem Schlüsselparameter (p, q, pinv, sp, dp, sq, dq) um ein Vielfaches des Sicherungswertes (sp, sq) unterscheidet, glatt durch den Sicherungswert (sp, sq) teilbar ist.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch **gekennzeichnet**, daß bei der Integritätsüberprüfung eine mit den Schlüsselparametern (p, q, pinv, sp, dp, sq, dq) abgespeicherte Prüfsumme mit einer nach der Übergabe der Schlüsselparameter (p, q, pinv, sp, dp, sq, dq) neu berechneten Prüfsumme verglichen wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch **gekennzeichnet**, daß zur Prüfung der Integrität wichtige Übergabeparameter mehrfach übergeben und nach der Übergabe auf Identität geprüft werden.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch **gekennzeichnet**, daß die kryptographische Berechnung eine Entschlüsselung oder Signaturerzeugung gemäß einem RSA-Verfahren, insbesondere einem RSA-CRT-Verfahren, ist.

8. Verfahren nach Anspruch 7, dadurch **gekennzeichnet**, daß bei der kryptographischen Berechnung mindestens eine Potenzierungsoperation durchgeführt wird, und daß bei der Integritätsprüfung (30, 34, 40, 54) geprüft wird, ob der bei der Potenzierungsopera-

tion verwendete Exponent sich als glatter Quotient einer Division eines Wertes durch einen Sicherungswert (sp, sq) ergibt.

9. Verfahren nach Anspruch 8, dadurch **gekennzeichnet**, daß bei der kryptographischen Berechnung ein Exponenten-Verschleierungsverfahren zum Ausspähungsschutz angewendet wird.

10. Verfahren nach einem der Ansprüche 7 bis 9, dadurch **gekennzeichnet**, daß die Primfaktoren (p, q) des RSA-Verfahrens mit einem Verschleierungsparameter (j) multipliziert werden, und daß die Fehlerfreiheit des Berechnungsverlaufs durch eine Gleichheitsüberprüfung modulo des Verschleierungsparameters (j) überprüft wird.

11. Verfahren zum Bestimmen eines Schlüssels für eine kryptographische Berechnung mit mindestens zwei Schlüsselparametern (p, q, pinv, sp, dp, sq, dq), wobei der Schlüssel zur Verwendung in einem Verfahren nach einem der Ansprüche 1 bis 10 vorgesehen ist.

12. Computerprogrammprodukt, das Programmbefehle aufweist, um einen Prozessor zu veranlassen, ein Verfahren mit den Merkmalen eines der Ansprüche 1 bis 11 auszuführen.

13. Tragbarer Datenträger, insbesondere Chipkarte oder Chipmodul, der zur Ausführung eines Verfahrens mit den Merkmalen eines der Ansprüche 1 bis 11 eingerichtet ist.